CLAIMS

WHAT IS CLAIMED IS:

1. A method of detecting states that are activated by a computer unit, the method comprising:

checking a set of values in a memory area of the computer unit or in a proprietary file within stored within the computer unit, with each set of values correspond to a state activated by the computer unit; and

capturing each set of values to determine each state activated by the computer unit.

2. The method of claim 2 wherein the checking the set of values comprises:

initiating a parallel registry segment thread.

3. The method of claim 2 wherein the initiating the parallel registry segment thread comprises:

collecting registry data.

4. The method of claim 1 wherein the checking the set of values comprises:

initiating a parallel operating system segment thread.

5. The method of claim 4 wherein the initiating the parallel operating system segment thread comprises:

analyzing at least one of an operating system directory structure, "root" and all directories and sub-directories.

6. The method of claim 1 wherein the checking the set of values comprises:

initiating a parallel third party segment thread.

7. The method of claim 6 wherein the initiating the parallel third party segment thread comprises:

scanning all third party start up files and all initialization files.

8. The method of claim 1 wherein the checking the set of values comprises:

initiating a polling thread.

9. The method of claim 8 wherein the initiating the polling thread comprises:

loading configuration data into memory.

10. The method of claim 8 wherein the initiating the polling thread comprises:

loading stored directory configuration data to memory.

11. The method of claim 8 wherein the initiating the polling thread comprises:

loading third party start up information into memory.

12. The method of claim 8 wherein the initiating the polling thread comprises:

detecting for an unauthorized modification.

13. The method of claim 1 further comprising:

transmitting each set of values to a remote computing unit.

14. An article of manufacture, comprising:

a machine-readable medium having stored thereon instructions to:

check a set of values in a memory area of the computer unit or in a proprietary file within stored within the computer unit, with each set of values correspond to a state activated by the computer unit; and

capture each set of values to determine each state activated by the computer unit.

15. An apparatus for detecting states that are activated by a computer unit, the apparatus comprising:

means for checking a set of values in a memory area of the computer unit or in a proprietary file within stored within the computer unit, with each set of values correspond to a state activated by the computer unit; and

communicatively coupled to the checking means, means for capturing each set of values to determine each state activated by the computer unit.

16. A method of electronically mapping the hard drive a computer unit to record an operating system and third-party application start-up environment, the method comprising:

(a) analyzing a memory for a presence of all critical directories and files;

(b) recording vital statistics of selected information;

(c) recording vital statistics for each critical file; and

(d) recording vital statistics of an internal registry in the computer unit.

17. The method of claim 16 wherein each of steps (a) through (d) are performed in real time.

18. A method of detecting states that are activated in an internal computer unit environment, the method comprising:

(a) monitoring an active window task manager for all identifiable window handles;

(b) intercepting operating system messages which are transmitted between a third-party application and an operating system;

(c) detecting change in a critical operating system file or third-party start-up file;

(d) detecting change in a critical aspect of a registry in the internal computer unit environment;

(e) sending a inner-process communications message to any identifiable window handle which resides within the active task manager;

(f) sending a real time forensic report to a monitor station, the real time forensic report defining the state of the detection.

19. A method of processing computer registry information, comprising:

storing all computer registry information in memory; and

recording the computer registry information into a structured file for transmission.

20. A method of checking all computer registry information in a real-time environment, the method comprising:

comparing the current computer unit machine registry activity state to the previously recorded registry state to detect unauthorized changes to a registry of the computer unit.

21. A method of storing electronically mapped directories and files, comprising:

providing electronically mapped directories which are required for the start-up of third-party applications installed within a computer unit; and

mapping the directories into a structured file.

22. A method of checking computer start-up directories and files, comprising:

comparing the current computer unit machine directory and file activity state to the previously recorded directory and file state to detect unauthorized changes to start-up directory and files of a computer unit.

23. A method of monitoring operating system (O/S) messages, comprising:

comparing messages to an authorized activity listing file to detect unauthorized activity.

24. A method of reporting the unauthorized internal activity in the computer unit, comprising:

detecting the unauthorized activity; and

transmitting a report of the activity to a second computer unit.

25. A method of detecting unauthorized activity in a computer unit, comprising

reporting an active focus window handle, in a real-time environment, by comparing the by comparing the messages to an authorized activity listing file, to detect unauthorized activity.

26. An apparatus for detecting states that are activated by a computer unit, the apparatus comprising:

a first engine capable to checking a set of values in a memory area of the computer unit or in a proprietary file within stored within the computer unit, with each set of values correspond to a state activated by the computer unit; and

communicative coupled to first engine, a second engine capable to capture each set of values to determine each state activated by the computer unit.

27. The apparatus of claim 26 wherein each state corresponds to a particular activity initiated the computer unit.

28. The apparatus of claim 26 wherein the first engine initiates a parallel registry segment thread.

29. The apparatus of claim 29 wherein the parallel registry segment thread is capable to collect registry data.

30. The apparatus of claim 26 wherein the first engine initiates a parallel operating system segment thread.

31. The apparatus of claim 30 wherein the parallel operating system segment thread is capable to analyze at least one of an operating system directory structure, "root" and all directories and sub-directories.

32. The apparatus of claim 26 wherein the first engine initiates a parallel third party segment thread.

33. The apparatus of claim 26 wherein the parallel third party segment thread is capable to scan all third party start up files and all initialization files.

34. The apparatus of claim 26 wherein the first engine initiates a polling thread.

35. The apparatus of claim 34 wherein the polling thread is capable to load configuration data into memory.

36. The apparatus of claim 34 wherein the polling thread is capable to load stored directory configuration data to memory.

37. The apparatus of claim 34 wherein the polling thread comprises is capable to load third party start up information into memory.

38. The apparatus of claim 34 wherein the polling thread is capable to detect for an unauthorized modification.

39. The apparatus of claim 26 further comprising:

a third engine capable to transmit each set of values to a remote computing unit.